REMARKS

The Examiner is thanked for the performance of a thorough search and for considering the references included in the Information Disclosure Statements filed on November 14, 2007 and June 13, 2007.

No claims have been amended, added, or canceled. Hence, Claims 1-2, 4, 6, 10, 12, 15-16, 20, 23-24, 31, 34, 38, 42, 47-48, 51, 54-56, 59, and 81-122 are currently pending in the application.

Each issue raised in the Office Action mailed December 13, 2007 is addressed hereinafter.

I. ISSUES RELATING TO THE CITED ART

A. INDEPENDENT CLAIM 1

Claim 1 was rejected under 35 U.S.C. § 102(e) as allegedly anticipated by Peyravian et al., U.S. Patent No. 6,363,154 ("PEYRAVIAN"). The rejection is respectfully traversed.

Claim 1 comprises the features of:

…;
the plurality of multicast proxy service nodes are logically represented by **a first binary tree**, wherein:
each node of the first binary tree is associated with a domain of a plurality of domains of a directory service that is distributed across the wide area network;
…;
creating and storing **a second binary tree** that represents the plurality of member nodes, wherein:
the second binary tree is stored in a particular domain of the plurality of domains of the directory service that is distributed across the wide area network;
…;
when an additional member node joins the multicast group, determining a new group session key by **replicating a branch of the second binary tree**.

PEYRAVIAN does not describe or suggest the above features of Claim 1.

1. PEYRAVIAN does not describe or suggest the feature of Claim 1 of determining a new group session key by replicating a branch of the

second binary tree when an additional member node joins the multicast group.

The Office Action asserts that the above feature of Claim 1 is described in col. 6, lines 43-67 of PEYRAVIAN. This assertion is incorrect.

In general, PEYRAVIAN describes a system and method for sending secure messages from a group of nodes (which are connected in a network) by defining a secret key at any one of the nodes. A message is encrypted at any one of the nodes with a session key that is generated from the secret key. The encrypted message is sent to the remaining nodes of the group. (See PEYRAVIAN, col. 2, lines 41-51.) The PEYRAVIAN system does not use a centralized group key distribution center; rather, only the member nodes of the group may generate and distribute group keys. This allows the nodes in the group to send secure messages without having to send the session key to each individual node. (See PEYRAVIAN, col. 2, lines 54-63.)

Significantly, however, PEYRAVIAN does not describe or suggest that a new group session key is determined by replicating a branch of a binary tree. On the contrary. In col. 2, line 67 to col. 3, line 17, PEYRAVIAN expressly describes that a working key, which a particular node may use to decrypt messages received from other nodes, is generated by computing a one-way hash from a random secret key (which is received from a first node) and from a random number (which is received from a second node). There is absolutely nothing in PEYRAVIAN that describes or suggests determining a session key by replicating a branch of a binary tree.

In col. 6, lines 43-67, PEYRAVIAN describes that a secret key K may be distributed to the member nodes of a group in several different ways. In one way, the node sending the secret key K may encrypt K under the public key of the receiving node and sign this

encrypted value using the sending node's private signature-generating key. (See PEYRAVIAN, col. 6, lines 44-47.) In another way, the node sending the secret key K may use a conventional Diffie-Hellman key establishment protocol to first establish a common shared key with the receiving node and then encrypt K with this shared secret key. (See PEYRAVIAN, col. 6, lines 48-52.) Significantly, however, PEYRAVIAN does not describe that any form of replication may be used to distribute a new session key when a new node joins the group of nodes.

In contrast, Claim 1 comprises the feature of determining a new group session key by **replicating a branch of the second binary tree** when an additional member node joins the multicast group. Neither the above passages nor any other passage from PEYRAVIAN describes or suggests that replication is used in determining a new session key.

For the above reasons, PEYRAVIAN does not describe or suggest the feature of Claim 1 of determining a new group session key by replicating a branch of the second binary tree when an additional member node joins the multicast group.

2. PEYRAVIAN does not describe or suggest the features of Claim 1 of: (1) representing a plurality of multicast proxy service nodes in a first binary tree, where each node of the first binary tree is associated with a domain of a plurality of domains of a directory service that is distributed across a wide-area network; and (2) creating and storing a second binary tree in a particular domain of the plurality of domains, where the second binary tree represents the plurality of member nodes.

PEYRAVIAN does not describe or suggest the above features of Claim 1. There is absolutely nothing in PEYRAVIAN that describes or suggests **a directory service** and a **plurality of domains** of the directory service. The Office Action asserts that the above

features of Claim 1 are described in col. 6, lines 13-67 of PEYRAVIAN. This assertion is incorrect.

In col. 6, lines 13-42, PEYRAVIAN distinguishes its system from RFC 1949, ANSI X9.69, and RFC 2093. Specifically, the passage in col. 6, lines 13-42 describes that: (1) in contrast to RFC 1949, the PEYRAVIAN system does not include a key distribution center; (2) in contrast to ANSI X9.69, PEYRAVIAN does not include a domain authority or a group manager node; and (3) in contrast to RFC 2093, PEYRAVIAN does not use a group controller to establish session keys. Further, in col. 6, lines 43-67, PEYRAVIAN describes that a secret key may be distributed to the member nodes of a group in several different ways, which include encryption with public/private keys of the sending/receiving nodes and encryption with shared keys that are established by using a conventional Diffie-Hellman protocol. Significantly, neither col. 6, lines 13-67 nor any other passage in PEYRAVIAN describes or suggests a directory service and a plurality of domains associated therewith. If anything, by distinguishing RFC 1949, ANSI X9.69, and RFC 2093, PEYRAVIAN expressly teaches against using any domain authority, key distribution center, group controller, and any other type of a group manager node.

In contrast, Claim 1 comprises the features of: (1) representing a plurality of multicast proxy service nodes in a first binary tree, **where each node of the first binary tree is associated with a domain of a plurality of domains of a directory service** that is distributed across a wide-area network; and (2) **creating and storing a second binary tree in a particular domain** of the plurality of domains, where the second binary tree represents the plurality of member nodes.

For the reasons given above, PEYRAVIAN does not describe or suggest all features of Claim 1. Thus, Claim 1 is patentable under 35 U.S.C. § 102(e) over PEYRAVIAN. Reconsideration and withdrawal of the rejection of Claim 1 is respectfully requested.

B. INDEPENDENT CLAIMS 59, 81, AND 102

Claims 59, 81, and 102 were rejected under 35 U.S.C. § 102(e) as allegedly anticipated by PEYRAVIAN.

Claims 59, 81, and 102 include features similar to the features of Claim 1 discussed above. Thus, Claims 59, 81, and 102 are patentable under 35 U.S.C. § 102(e) over PEYRAVIAN for at least the reasons given above with respect to Claim 1. Reconsideration and withdrawal of the rejections of Claims 59, 81, and 102 is respectfully requested.

C. DEPENDENT CLAIMS 2, 4, 6, 10, 12, 15-16, 20, 23-24, 31, 34, 38, 42, 47-48, 51, 54-56, 82-101, and 103-122

Claims 2, 4, 6, 10, 12, 15-16, 20, 23-24, 31, 34, 38, 42, 47-48, 51, 54-56, 82-101, and 103-122 were rejected under 35 U.S.C. § 102(e) as allegedly anticipated by PEYRAVIAN.

Each of Claims 2, 4, 6, 10, 12, 15-16, 20, 23-24, 31, 34, 38, 42, 47-48, 51, 54-56, 82-101, and 103-122 depends from one of independent Claims 1, 81, and 102, and thus includes each and every feature of the independent base claim. In addition, each of Claims 2, 4, 6, 10, 12, 15-16, 20, 23-24, 31, 34, 38, 42, 47-48, 51, 54-56, 82-101, and 103-122 introduces one or more additional features that independently render it patentable. However, due to the fundamental differences already identified, to expedite the positive resolution of this application a separate discussion of those features is not included at this time. Therefore, it is respectfully submitted that Claims 2, 4, 6, 10, 12, 15-16, 20, 23-24, 31, 34, 38, 42, 47-48, 51, 54-56, 82-101, and 103-122 are allowable for the reasons given above with respect to Claims 1, 81, and 102. Reconsideration and withdrawal of the rejections of Claims 2, 4, 6,

10, 12, 15-16, 20, 23-24, 31, 34, 38, 42, 47-48, 51, 54-56, 82-101, and 103-122 is respectfully requested.

II. CONCLUSION

The Applicant believes that all issues raised in the Office Action have been addressed. Further, for the reasons set forth above, the Applicant respectfully submits that allowance of the pending claims is appropriate. Reconsideration of the present application is respectfully requested in light of the remarks herein.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

A petition for extension of time, to the extent necessary to make this reply timely filed, is hereby made. If applicable, a law firms check for the petition for extension of time fee is enclosed herewith. If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to charge any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Dated: February 21, 2008

/StoychoDDraganoff#56181/
Stoycho D. Draganoff
Reg. No. 56,181

2055 Gateway Place, Suite 550
San Jose, California 95110-1089
Telephone No.: (408) 414-1080 ext. 208
Facsimile No.: (408) 414-1076